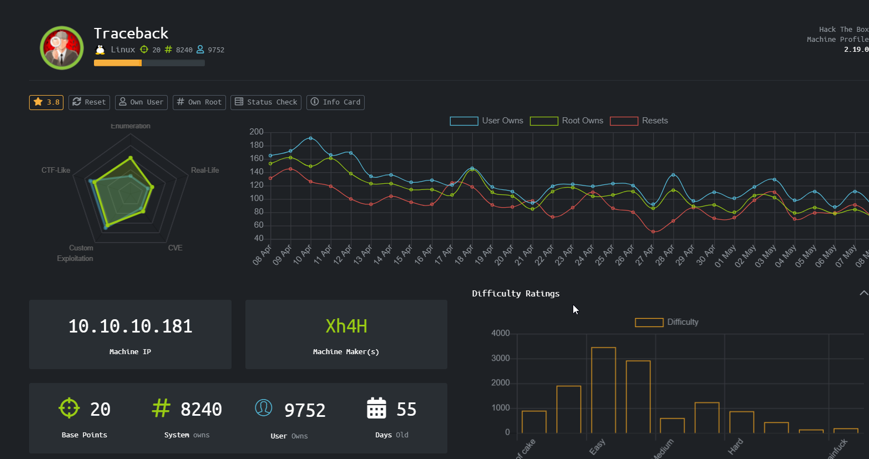
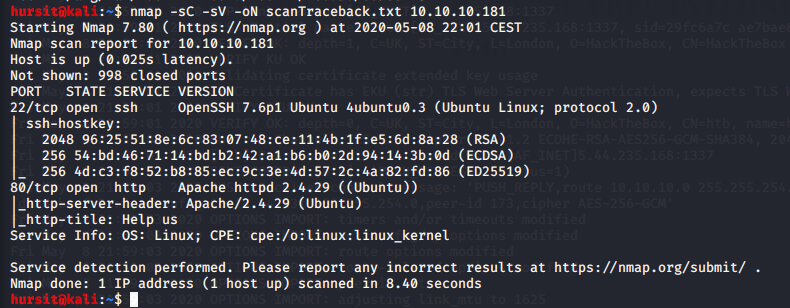
**Red Teaming Aspect: Ethical Hacking**

**Level A+ Requirements:**

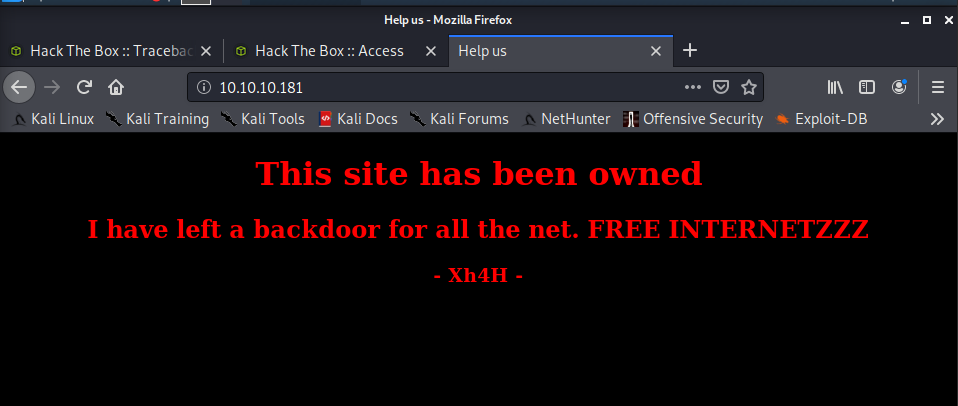
Nu moeten we een actieve machine hacken, ik heb gekozen voor de machine ‘Traceback’. Een linux machine met IP 10.10.10.181. 

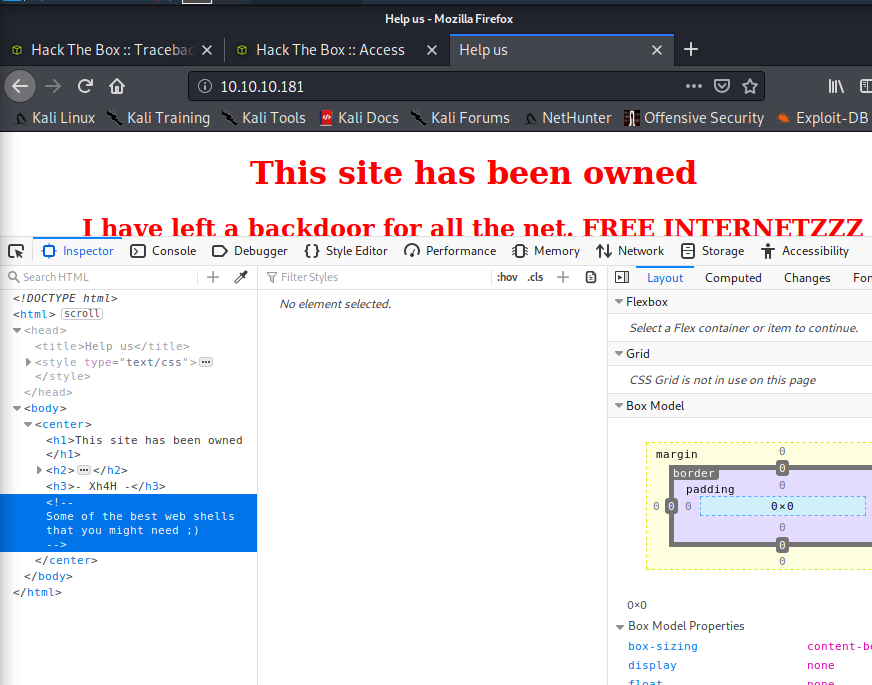
Zoals bij requirement b gaan we eerst een nmap scan uitvoeren.



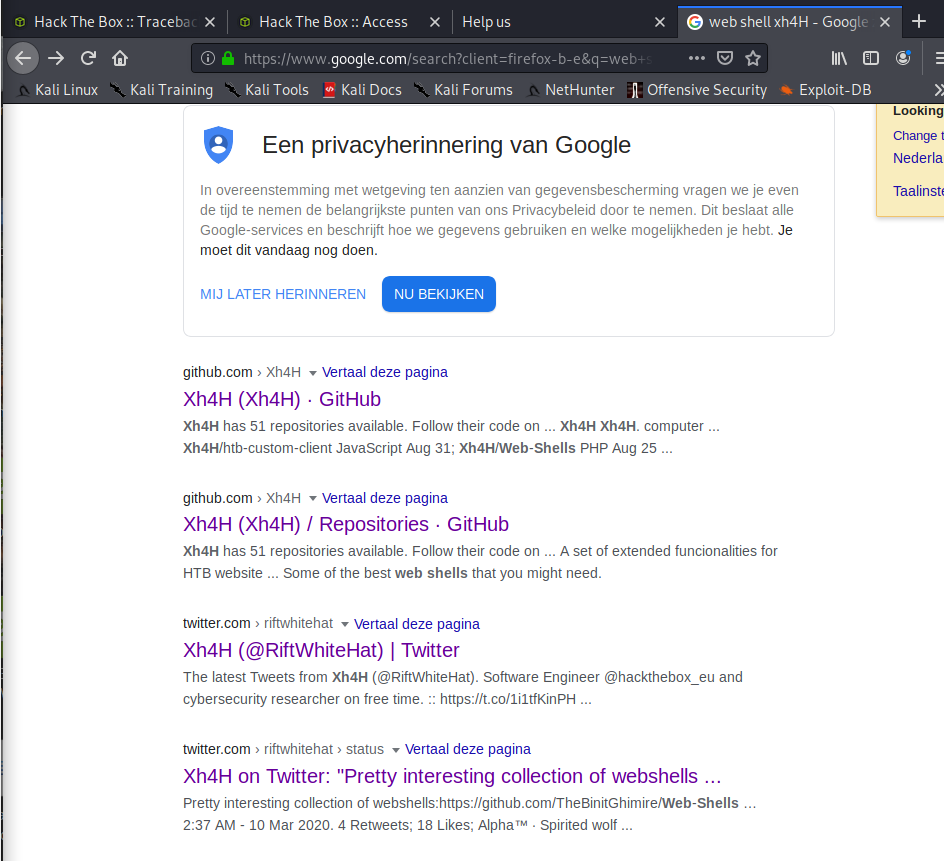
We zien poort 22 en poort 80.

Wanneer we gaan kijken in onze webbrowser zien we het volgende:

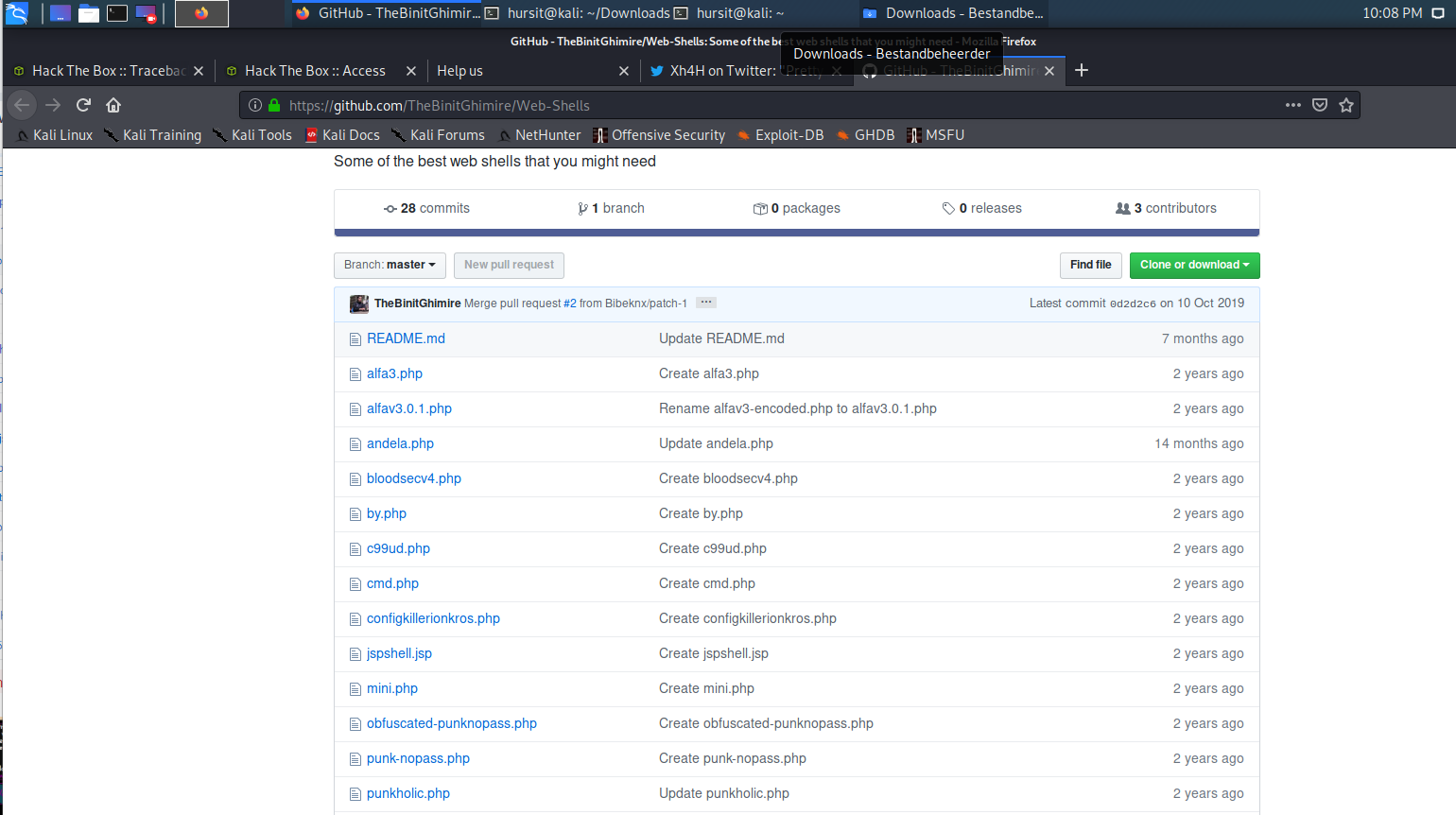




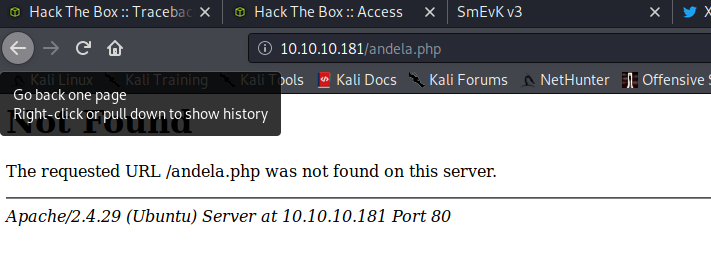
De maker heeft voor ons een tip achtergelaten in comment.

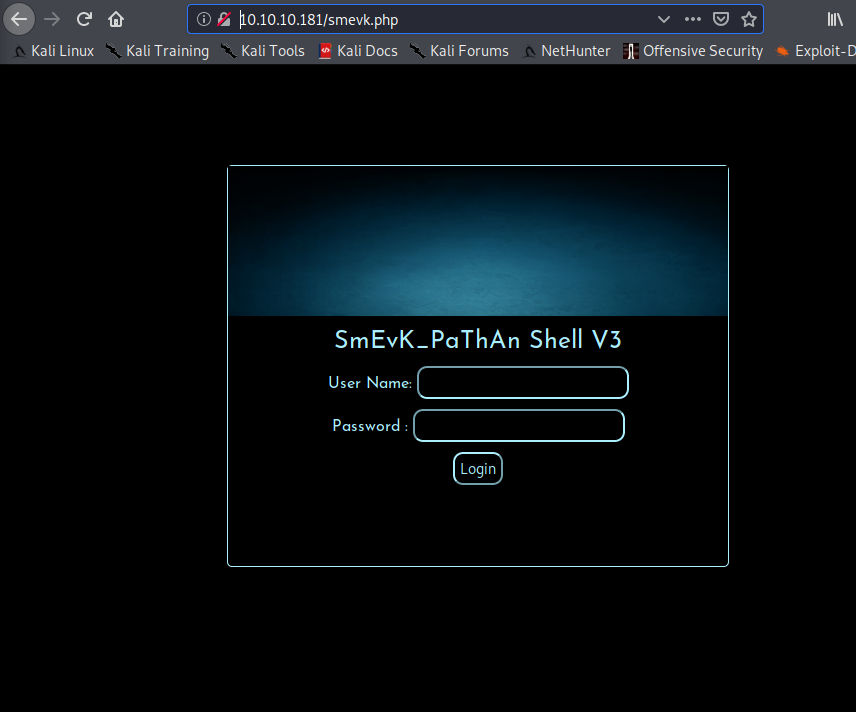


Als we ‘Some of the best web shells’ opzoeken dan krijgen we een git repository en een Twitter-account, allebij met de naam van de maker van de machine. De tweet is niks speciaal, het is een link naar github, dus ik wist dat ik op het juiste spoor was.

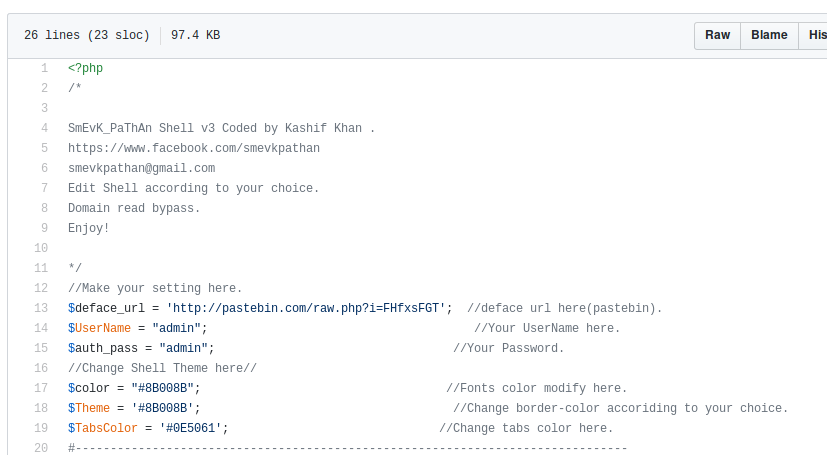


Op github zag ik allemaal verschillende files. Deze heb ik allemaal uitgeprobeert in mijn browser tot ik een werkende tegenkwam.

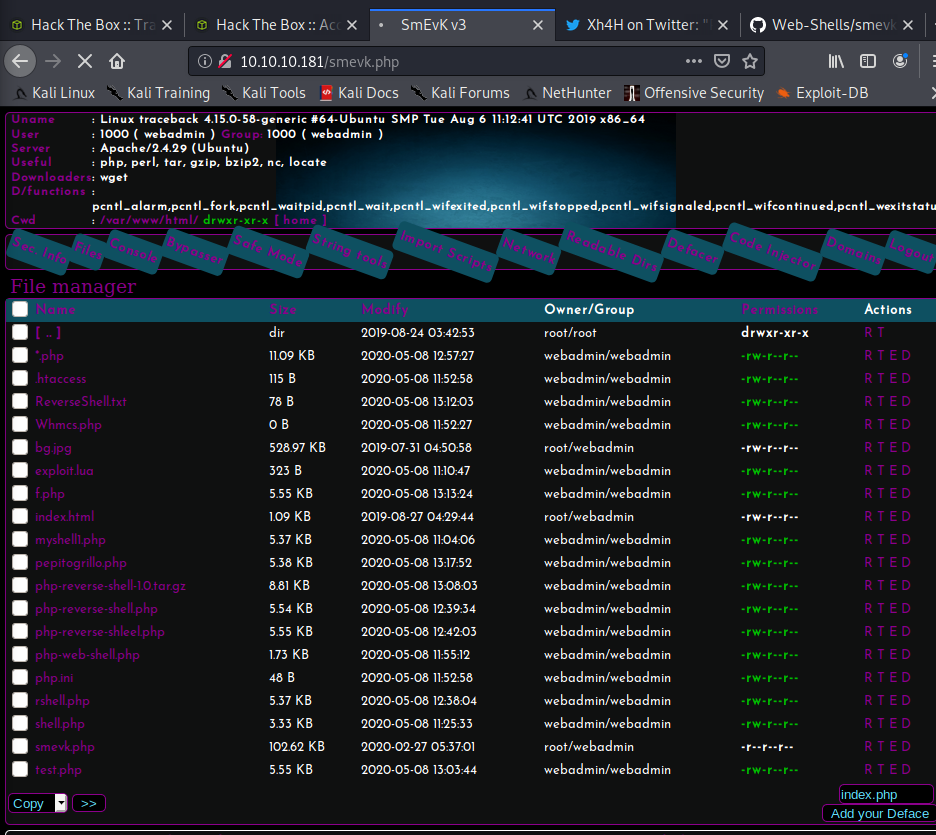




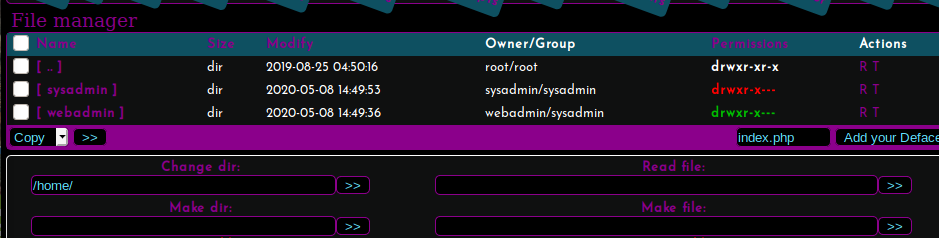
Bij smevk.php kreeg ik een loginscherm. Als ik nu bij github het script bekeek zag ik dat login en passwoord allebij ‘admin’ waren.



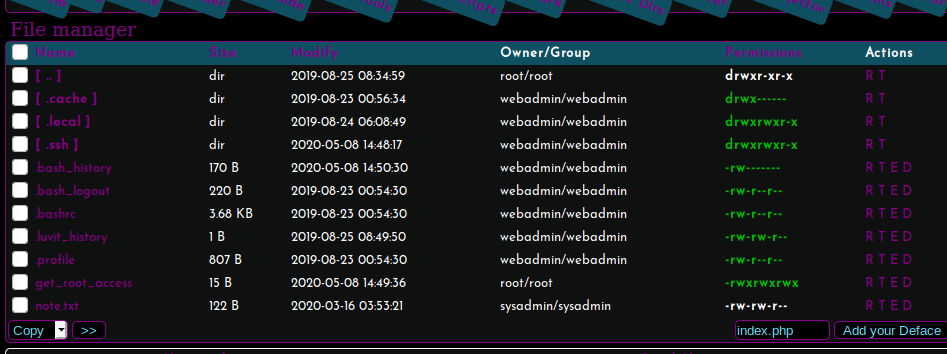
Na het inloggen krijgen we volgend scherm:



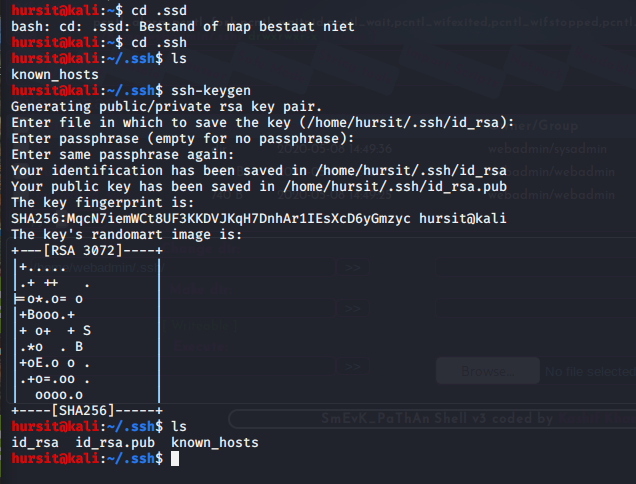
Na wat zoeken en kijken kwam ik bij de home folder waarbij ik sysadmin en wabadmin directories zag.

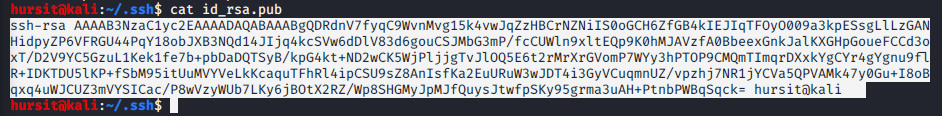


We hadden de machtigingen om in webadmin te geraken maar geen access tot sysadmin.

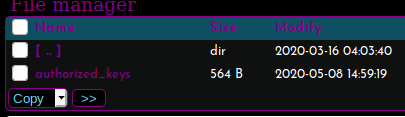
Dit is wat we zien in webadmin: 

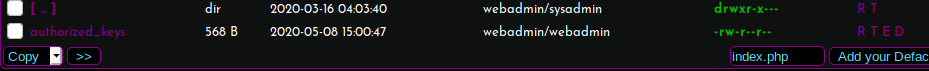
Bij de .ssh directory is er een file die authorized\_keys noemt. Dit zorgt ervoor dat we kunnen inloggen zonder een passwoord nodig te hebben. Na wat zoeken op het internet heb ik gezien dat we dit heel makkelijk kunne omzeilen. Via mijn eigen terminal heb ik een ssh key gegenereerd. Deze key heb ik dan in een file geplakt met dezelfde naam.



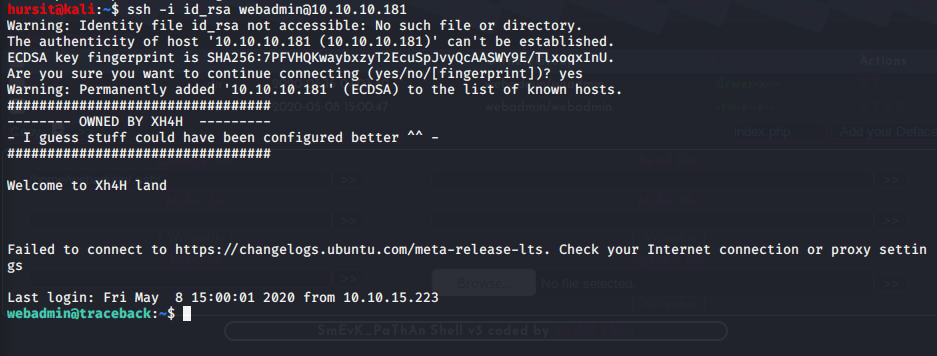


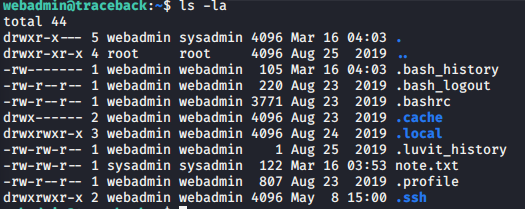
Daarna heb ik het bestaande bestand veranderd door mijn bestand, waardoor mij ssh key nu in authorized\_keys staat.



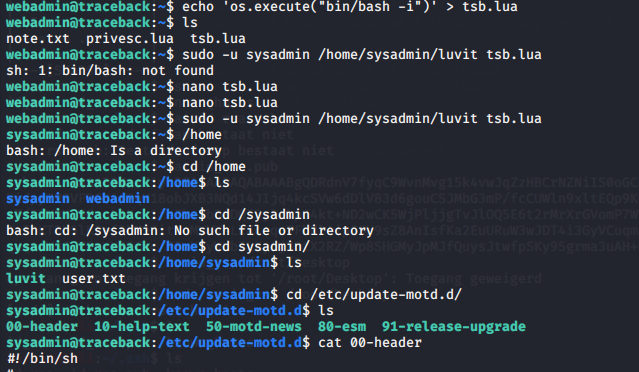


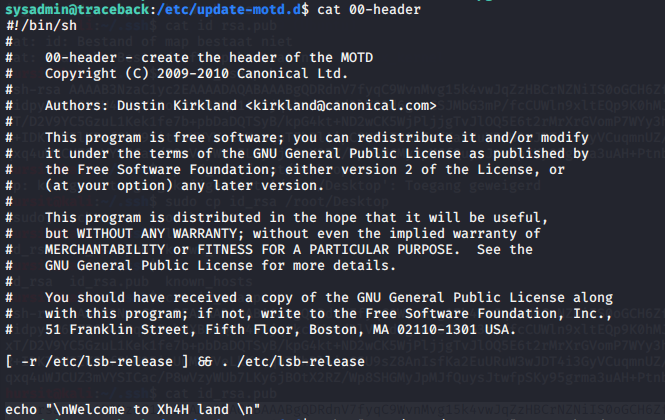
Nu kunnen we verbinding maken via onze eigen terminal met het volgende commando:



Als we nu ls doen zien we alle files, zonder -la zien we enkel note.txt. 

In de .txt staat gegeven dat de maker ons een tool heeft achtergelaten om Lua te oefenen. Met behulp van Lua gaan we kunnen switchen naar sysadmin. Zoals in de volgende afbeelding.

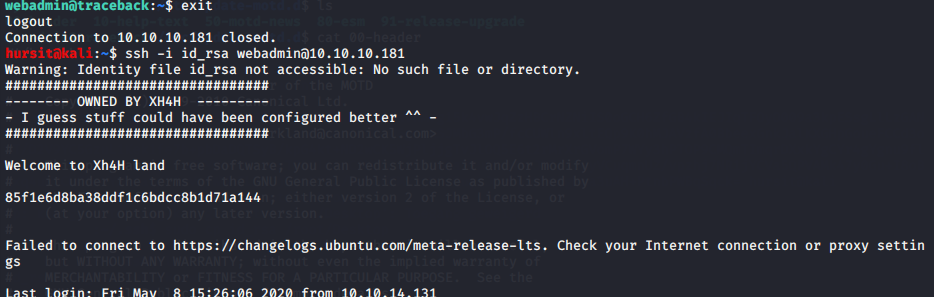


Als we ls doen op sysadmin dan zien we 00-header staan, laten we dit even openen. 

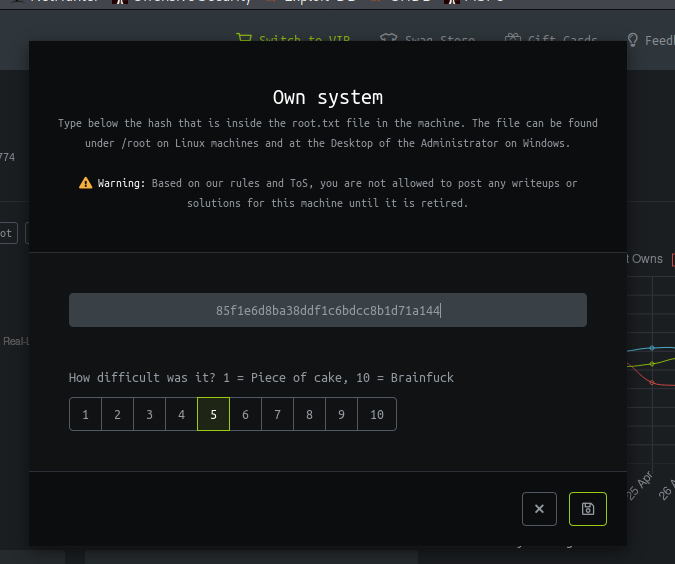
We gaan ervoor zorgen dat we de flag voor root access via de header kunnen bekijken.



We gaan nu even opnieuw inloggen om de motd te bekijken.



Hier zien we de key voor Own System.



Voor Own User gaan we nu een nieuwe sessie opstarten, weer hetzelfde proces als hiervoor dus ook een nieuwe ssh key. We gaan weer gebruik maken van een .lua file. We gaan het commando ‘os.execute(“/bin/sh”)’ uitvoeren en dit wegschrijven naar een .lui file. Daarna gaan we een sessie opstarten aks sysadmin en via daar user.txt openen.

